Hard Drives and Hard Ethical Issues

Some Legal, Ethical and Practical Concerns for Prosecutors Conducting Their Own Searches of Digital Storage Media

Eric Klumb
Trial Attorney
Computer Crime and Intellectual Property Section
October 2003

I. Potentially Applicable Rules: ABA Model Rules of Professional Conduct (2001)

A. Rule 3.7 Lawyer as Witness

(a) A lawyer shall not act as advocate at a trial in which the lawyer is likely to be a necessary witness except where:

(1) the testimony relates to an uncontested issue;
(2) the testimony relates to the nature and value of legal services rendered in the case; or
(3) disqualification of the lawyer would work substantial hardship on the client.

(b) A lawyer may act as advocate in a trial in which another lawyer in the lawyer's firm is likely to be called as a witness unless precluded from doing so by Rule 1.7 or Rule 1.9 .

B. Rule 3.8 Special Responsibilities of a Prosecutor

The prosecutor in a criminal case shall:
(a) refrain from prosecuting a charge that the prosecutor knows is not supported by probable cause;
(b) make reasonable efforts to assure that the accused has been advised of the right to, and the procedure for obtaining, counsel and has been given reasonable opportunity to obtain counsel;
(c) not seek to obtain from an unrepresented accused a waiver of important pretrial rights, such as the right to a preliminary hearing;
(d) make timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense, and in connection with sentencing, disclose to the defense and to the tribunal all unprivileged mitigating information known to the prosecutor, except when the prosecutor is relieved of this responsibility by a protective order of the tribunal;
(e) exercise reasonable care to prevent investigators, law enforcement personnel, employees or other persons assisting or associated with the prosecutor in a criminal case from making an extrajudicial statement that the prosecutor would be prohibited from making under Rule 3.6 ;
(f) not subpoena a lawyer in a grand jury or other criminal proceeding to present evidence about a past or present client unless the prosecutor reasonably believes :

(i) the information sought is not protected from disclosure by any applicable privilege;
(ii) the evidence sought is essential to the successful completion of an ongoing investigation or prosecution; and
(iii) there is no other feasible alternative to obtain the information;

(g) except for statements that are necessary to inform the public of the nature and

extent of the prosecutor's action and that serve a legitimate law enforcement purpose, refrain from making extrajudicial comments that have a substantial likelihood of heightening public condemnation of the accused.

C. Rule 4.4 Respect for Rights of Third Persons

In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

II. Search Issues and Rule 4.4

A. Exceeding the scope of the warrant

1. Whether specifically authorized by the warrant or not, agents often seize storage media containing numerous files outside the scope of the warrant, to be searched later off-site. Due to the practical problems involved in completing on-site searches of digital media for materials particularly described in the warrant, this practice is permissible. *See, e.g., Davis v. Gracey*, 111 F.3d 1472, 1280 (10th Cir. 1997) (noting "the obvious difficulties attendant in separating the contents of electronic storage [sought as evidence] from the computer hardware [seized] during the course of a search"); *United States v. Schandl*, 947 F.2d 462, 465-466 (11th Cir. 1991) (noting that an on-site search "might have been far more disruptive" than the off-site search conducted); *United States v. Henson*, 848 F.2d 1374, 1383-84 (6th Cir. 1988) ("We do not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the [defendant's] office, in an effort to segregate those few papers that were outside the warrant."); *United States v. Scott-Emuakpor*, 2000 WL 288443, at *7 (W.D. Mich. Jan. 25, 2000) (noting "the specific problems associated with conducting a search for computerized records" that justify an off-site search); *United States v. Gawrysiak*, 972 F. Supp. 853, 866 (D.N.J. 1997), aff'd, 178 F.3d 1281 (3d Cir. 1999), ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant."); *United States v. Sissler*, 1991 WL 239000, at *4 (W.D. Mich. Jan. 25, 1991) ("The police . . . were not obligated to inspect the computer and disks at the . . . residence because passwords and other security devices are often used to protect the information stored in them. Obviously, the police were permitted to remove them from the . . . residence so that a computer expert could attempt to 'crack' these security measures, a process that takes some time and effort. Like the seizure of

documents, the seizure of the computer hardware and software was motivated by considerations of practicality. Therefore, the alleged carte blanche seizure of them was not a 'flagrant disregard' for the limitations of a search warrant."). *See also United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) ("It is no easy task to search a well-laden hard drive by going through all of the information it contains . . . . The record shows that the mechanics of the search for images later performed [off-site] could not readily have been done on the spot."); *United States v. Lamb*, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) ("[I]f some of the image files are stored on the internal hard drive of the computer, removing the computer to an FBI office or lab is likely to be the only practical way of examining its contents.").

2. The prosecutor who examines a duplicate image of seized media is not just reviewing copies of materials already seized and searched by the agents executing the warrant; *the prosecutor may be conducting the search itself!* Query: Is an AUSA an officer authorized to execute the warrant within the meaning of Rule 41(c)(1) and 18 U.S.C. § 3105? Suppression may not be a problem, *see United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (rule and statute violations in execution of the warrant justifies suppression only if there is a corresponding 4th Amendment violation), but the ethical issue remains.

3. A reviewing prosecutor unskilled at utilizing the search software may inadvertently exceed the scope of the search; a trained forensic examiner may be able to stay within the warrant's scope. Violations of the scope of the warrant may result in the suppression. *See United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (warrant authorized search of computer for evidence of drug dealing, but the officer came across child pornography and then continued to look for it, resulting in suppression of the pornography). Some courts state that an examiner may look at every file to determine whether it falls within the warrant, but the fact that the examiner sought a second warrant after plain view discovery will defeat suppression. *United States v. Triumph Capital Group*, Inc,. 211 F.R.D. 31, 62 (D. Conn. 2002)(agent "not required to assume that document and file names and suffixes accurately described their contents, and he acted reasonably in manually reviewing documents and files to ascertain their relevance"); *United States v. Gray*, 78 F.Supp. 524, 529, n. 8 (E.D. Va. 1999)(agent "entitled to look at all of defendant's files to determine whether they fell within the scope of the warrant" even though there may have been more technically advanced methods of limiting the search).

4. Typically, however, only the items outside the scope will be suppressed. *See, e.g., United States v. Hargus*, 128 F.3d 1358, 1363 (10th Cir. 1997). To be entitled to blanket suppression, the defendant must establish that the

warrant was executed in "flagrant disregard" of its terms. *See, e.g., United States v. Le*, 173 F.3d 1258, 1269 (10th Cir. 1999); *United States v. Matias*, 836 F.2d 744, 747-48 (2d Cir. 1988) (citing cases). A search is executed in "flagrant disregard" of its terms when the officers so grossly exceed the scope of the warrant during execution that the authorized search appears to be merely a pretext for a "fishing expedition" through the target's private property. See, e.g., *United States v. Liu*, 239 F.3d 138 (2d Cir. 2000); *United States v. Foster*, 100 F.3d 846, 851 (10th Cir. 1996); *United States v. Young*, 877 F.2d 1099, 1105-06 (1st Cir. 1989).

5. Even if no evidence is suppressed, a finding that the prosecutor's search exceeded the warrant's limits may result in a state ethics or OPR referral.

B. The Privacy Protection Act ("PPA")

1. Purpose is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

2. PPA makes it unlawful for a government officer "to search for or seize" materials when

   (a) the materials are "work product materials" prepared, produced, authored, or created "in anticipation of communicating such materials to the public," 42 U.S.C. § 2000aa-7(b)(1);

   (b) the materials include "mental impressions, conclusions, or theories" of its creator, 42 U.S.C. § 2000aa-7(b)(3); and

   (c) the materials are possessed for the purpose of communicating the material to the public by a person "reasonably believed to have a purpose to disseminate to the public" some form of "public communication," 42 U.S.C. §§ 2000aa-7(b)(3), 2000aa(a);

or

(a) the materials are "documentary materials" that contain "information," 42 U.S.C. § 2000aa-7(a); and

(b) the materials are possessed by a person "in connection with a purpose to disseminate to the public" some form of "public communication." 42 U.S.C. §§ 2000aa(b), 2000aa-7(a).

3. Exceptions

   a. Contraband, instrumentalities, or fruits of crime, 42 U.S.C. § 2000aa-7(a),(b);

   b. Death or bodily injury, 42 U.S.C. §§ 2000aa(a)(2), 2000aa(b)(2);

   c. Possessor as suspect, 42 U.S.C. §§ 2000aa(a)(1), 2000aa(b)(1); or

   d. Inadequacy of subpoena, 42 U.S.C. § 2000aa(b)(3)-(4).

4. Violations of the PPA do not result in suppression of the evidence, see 42 U.S.C. § 2000aa-6(d), but can result in civil damages against the sovereign whose officers or employees execute the search. See § 2000aa-6(a), (e); *Davis v. Gracey*, 111 F.3d 1472, 1482 (10th Cir. 1997) (dismissing PPA suit against municipal officers in their personal capacities because such suits must be filed only against the "government entity" unless the government entity has not waived sovereign immunity).

5. The incidental seizure of PPA-protected material commingled on a suspect's computer with evidence of a crime does not give rise to PPA liability. *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001). "[W]hen police execute a search warrant for documents on a computer, it will often be difficult or impossible (particularly without the cooperation of the owner) to separate the offending materials from other 'innocent' material on the computer" at the site of the search. Id. at 341-42. The *Guest* court cautioned, however, that although the incidental seizure of PPA-related work-product and documentary materials did not violate the Act, the subsequent *search* of such material was probably forbidden. *Id.*

6. Again, even though a prosecutor's search of PPA-protected material may not result in either suppression or personal liability, a finding that the act was violated may result in a state ethics or OPR referral.

III. **Lawyer-Witness Rule**

A. If a prosecutor's search of media finds an incriminating file, the file can be introduced through an agent who duplicates the search.

B. If the prosecutor has to testify at trial, it is likely that it will be permitted, but the prosecutor may be disqualified from presenting the case to the trier of fact. *See United States v. Edwards*, 154 F.3d 915, 923 (9th Cir 1998) ("[W]hen a prosecutor is personally involved in the discovery of a critical piece of evidence, when that fact is made evident to the jury, and when the reliability of the circumstances surrounding the discovery of the evidence is at issue, the prosecutor's participation in the trial of the defendant constitutes an improper form of vouching."); *United States v. Watson*, 87 F.3d 927, 932 (7th Cir. 1996) (suggesting that the correct way for an AUSA to avoid hitting the stand is to always have an agent present during witness interviews); *United States v McCrady*, 774 F.2d 868, 872 (8th Cir 1985) (AUSA not involved in the trial may testify about statement made by government witness during pretrial interview)*; United States v. Johnston*, 690 F.2d 638, 646 (7th Cir. 1982) (AUSA may testify at preliminary proceeding and represent the government at trial, where critical conversation between defendant and AUSA occurred when defendant called the prosecutor); *United States v. Bin Laden*, 91 F.Supp2d 600, 622-24 (S.D.N.Y. 2000) (defense attempt to use the lawyer-witness prohibition to disqualify AUSAs who interviewed witnesses rejected where AUSAs always conducted interviews in the presence of third parties).

1. Practice Pointer: If you do examine a copy of the storage media, keep a detailed audit log of the steps taken during the "search," in case an agent needs to duplicate the steps or in case your search itself is ever at issue.

CREDITS:

Paul Ohm of the Computer Crime and Intellectual Property Section, Criminal Division, provided helpful advice, and the Section's manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (July 2002) (available at www.cybercrime.gov) was flagrantly plagiarized.